provided, locked rooms or buildings normally provide adequate after-hours protection. If such protection is not considered adequate, DoD UCNI material shall be stored in locked receptacles; i.e., file cabinets, desks, or bookcases.

3. Nonrecord copies of DoD UCNI materials must be destroyed by tearing each copy into pieces to reasonably preclude reconstruction and placing the pieces in regular trash containers. If the sensitivity or volume of the information justifies it, DoD UCNI material may be destroyed in the same manner as classified material rather than by tearing. Record copies of DoD UCNI documents shall be disposed of, in accordance with the DoD Components' record management regulations. DoD UCNI on magnetic storage media shall be disposed of by overwriting to preclude its reconstruction.

4. The unauthorized disclosure of DoD UCNI material does not consititute disclosure of DoD information that is classified for security purposes. Such disclosure of DoD UCNI justifies investigative and administrative actions to determine cause, assess impact, and fix responsibility. The DoD Component that originated the DoD UCNI information shall be informed of its unauthorized disclosure and the outcome of the investigative and administrative actions.

G. Retirement of Document of Material

1. Any unclassified document or material which is not marked as containing DoD UCNI but which may contain DoD UCNI shall be marked upon retirement in accordance with the DoD Components' record management regulations.

2. A document or material marked as containing DoD UCNI is not required to be reviewed by a Reviewing Official upon or subsequent to retirement. A Reviewing Official shall review any retired document or material upon a request for its release made under 5 U.S.C. 552.

H. Requests for Public Release of DoD UCNI

DoD 5400.7–R applies. Information that qualifies as DoD UCNI, under 10 U.S.C. 128, is exempt from mandatory disclosure under 5 U.S.C. 552. Consequently, requests for the public release of DoD UCNI shall be denied under 5 U.S.C. 552(b)(3), citing 10 U.S.C. 128 as authority.

I. Reports

The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall prepare and maintain the quarterly reports required by 10 U.S.C. 128. The Heads of the DoD Components shall advise the ASD(C3I) when information not in the guidelines in appendix B to this part is determined to be DoD UCNI. Those reports shall have the following information:

1. Identification of the information to be controlled as DoD UCNI. It is not necessary to report each document or numbers of documents.

2. Justification for identifying the type of information to be controlled as DoD UCNI.

3. Certification that only the minimal information necessary to protect the health and safety of the public or the common defense and security is being controlled as DoD UCNI.

APPENDIX B TO PART 223—GUIDELINES FOR THE DETERMINATION OF DOD UCNI

A. Use of Determination of DoD UCNI Guidelines

1. These guidelines for determining DoD UCNI are the bases for determining what unclassified information about the physcial protection of DoD SNM, equipment or facilities in a given technical or programmatic subject area is DoD UCNI.

2. The decision to protect unclassified information as DoD UCNI shall be based on a determination that the unauthorized dissemination of such information could reasonably be expected to have an adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of SNM, equipment, or facilities.

B. General

1. The policy for protecting unclassified information about the physical protection of DoD SNM, equipment, or facilities is to protect the public's interest by controlling certain unclassified Government information so to prevent the adverse effects described in section D. of this appendix and in appendix A to this part, without restricting public availability of information that would not result in those adverse effects.

2. In controlling DoD SNM information, only the minimum restrictions needed to protect the health and safety of the public or the common defense and security shall be applied to prohibit the disclosure and dissemination of DoD UCNI.

3. Any material that has been, or is, widely and irretrievably disseminated into the public domain and whose dissemination was not, or is not, under Government control is exempt from control under these guidelines. However, the fact that information is in the public domain is not a sufficient basis for determining that similar or updated Government-owned and -controlled information in another document or material is not, or is no longer, DoD UCNI; case-by-case determinations are required.

C. Topical Guidance

The following elements of information shall be considered by the DoD Components during the preparation of unclassified information about the physical protection of DoD SNM to determine if it qualifies for control as DoD UCNI:

1. VULNERABILITY ASSESSMENTS

a. General vulnerabilities that could be associated with specific DoD SNM, equipment, or facility locations.

b. The fact that DoD SNM facility security-related projects or upgrades are planned or in progress.

c. Identification and description of security system components intended to mitigate the consequences of an accident or act of sabotage at a DoD SNM facility.

2. MATERIAL CONTROL AND ACCOUNTABILITY

a. Total quantity or categories of DoD SNM at a facility.

b. Control and accountability plans or procedures.

c. Receipts that, cumulatively, would reveal quantities and categories of DoD SNM of potential interest to an adversary.

d. Measured discards, decay losses, or losses due to fission and transmutation for a reporting period.

e. Frequency and schedule of DoD SNM inventories.

3. FACILITY DESCRIPTION

a. Maps, conceptual design, and construction drawings of a DoD SNM facility showing construction characteristics of building and associated electrical systems, barriers, and back-up power systems not observable from a public area.

b. Maps, plans, photographs, or drawings of man-made or natural features in a DoD SNM facility not observable from a public area; i.e., tunnels, storm or waste sewers, water intake and discharge conduits, or other features having the potential for concealing surreptitious movement.

4. INTRUSION DETECTION AND SECURITY ALARM SYSTEMS

a. Information on the layout or design of security and alarm systems at a specific DoD SNM facility, if the information is not observable from a public area.

b. The fact that a particular system make or model has been installed at a specific DoD SNM facility, if the information is not observable from a public area.

c. Performance characteristics of installed systems.

5. KEYS, LOCKS, COMBINATIONS, AND TAMPER-INDICATING DEVICES

a. Types and models of keys, locks, and combinations of locks used in DoD SNM facilities and during shipment.

b. Method of application of tamper-indicating devices.

c. Vulnerability information available from unclassified vendor specifications.

6. THREAT RESPONSE CAPABILITY AND PROCEDURES

a. Information about arrangements with local, State, and Federal law enforcement Agencies of potential interest to an adversary.

b. Information in ''nonhostile'' contingency plans of potential value to an adversary to defeat a security measure; i.e., fire, safety, nuclear accident, radiological release, or other administrative plans.

c. Required response time of security forces.

7. PHYSICAL SECURITY EVALUATIONS

a. Method of evaluating physical security measures not observable from public areas.

b. Procedures for inspecting and testing communications and security systems.

8. IN-TRANSIT SECURITY

a. Fact that a shipment is going to take place.

b. Specific means of protecting shipments.

c. Number and size of packages.

d. Mobile operating and communications procedures that could be exploited by an adversary.

e. Information on mode, routing, protection, communications, and operations that must be shared with law enforcement or other civil agencies, but not visible to the public.

f. Description and specifications of transport vehicle compartments or security systems not visible to the public.

9. INFORMATION ON NUCLEAR WEAPON STOCKPILE AND STORAGE REQUIREMENT, NUCLEAR WEAPON DESTRUCTION AND DISABLEMENT SYSTEMS, AND NUCLEAR WEAPONS PHYSICAL CHARACTERISTICS

Refer to CG-W-5 for guidance about the physical protection of information on nuclear weapon stockpile and storage requirements, nuclear weapon destruction and disablement systems, and nuclear weapon physical characteristics that may, under certain circumstances, be unclassified. Such information meets the adverse effects test shall be protected as DoD UCNI.